CHILD & ADULT CARE FOOD PROGRAM CTD REQUEST FORM

To Add/Change/Delete Sponsor or Site CTD(S) Codes

Check appropriate box *- one per form:*

☐ New Sponsor/District
Date Sponsor/District Opens: _____

☐ Add New Site
Date Site Opens: _____

☐ Delete Sponsor/District
Date Sponsor/District Deleted: _____

☐ Delete Site
Date Site Deleted: _____

☐ Change Data for Sponsor/District
Date of Change: _____

☐ Change Data for Site
Date of Change: _____

List CTD number *(* leave site code blank if adding new site):*

CTD(S) # - **C**ounty code _____ (2 digits) **T**ype code _____ (2 digits) **D**istrict code _____ (2 digits) **S**ite code ***** _____ (3 digits)

Complete remainder of form and fax *to number provided below:*

SPONSOR/DISTRICT NAME: _____

SITE NAME: _____

PHYSICAL ADDRESS: _____

CITY: _____ STATE: _____ ZIP CODE: _____

MAILING ADDRESS: _____

CITY: _____ STATE: _____ ZIP CODE: _____

PHONE: _____ FAX: _____

CONTACT INFORMATION:

NAME: _____

TITLE: _____

PHONE: _____ FAX: _____

E-MAIL ADDRESS: _____

AUTHORIZING SIGNATURE: _____
(Superintendent, Business Manager, Principal, or Director)

Fax to: Debra Scott at the Health and Nutrition Division at **(602) 542-3818.**
Please call (602) 542-8700 if you have any questions.

Management Information Systems

Acceptable Use Policy

The following policy covers the use of electronic communication networks and computer-based administrative applications of the Arizona Department of Education (ADE). This policy applies to all personnel using these intranet, extranet, internet, and administrative resources, including, but not limited to, officials and employees of schools, school districts, charter schools, and ADE.

Administrative applications may require the collection, storage, and transmission of sensitive, confidential, private, or proprietary information. Such information must be properly safeguarded at all times, and procedures to ensure its security must be adhered to. Such information should be accessible only to properly authorized personnel, and confidential or sensitive information must be securely encrypted during transmission over electronic communication networks.

Use of ADE electronic communication networks and computer-based administrative applications is limited exclusively to business related to ADE. Use for other purposes is not acceptable.

It is not acceptable to use ADE intranet, extranet, internet, and administrative resources for any purposes which violate U.S. or state laws. It is not acceptable to use these resources so as to interfere with or disrupt network users, services or equipment. Users agree to waive any claim and release ADE, its employees, and agents, from any claim, demand, liability, cause of action, or suit for damages arising out of use of ADE resources, including but not limited to any loss of stored data. Users understand and agree that each time they access ADE resources, they are bound by the terms of this agreement along with any changes or additions to this agreement and the terms of all ADE policies that are in effect at the time they access the system

Use of ADE resources constitutes acceptance by the user of the terms of this agreement.

Ownership of Internet-Related systems

ADE Internet-related administrative application systems are the property of the Arizona Department of Education. They are to be used for business purposes in serving the interests of the ADE and its clients and in the course of normal operations.

Monitoring

ADE reserves the right to monitor all usage to ensure proper working order, appropriate use, the security of data, and to retrieve the contents of any user communication in these systems.

Security and Proprietary Information

Information contained on ADE's Internet-related systems may be either public information or non-public information. Users are required to take all necessary steps to prevent unauthorized access to or disclosure of non-public information.

Access and Authentication

Users are required to keep their passwords secure and unknown to all other persons and shall not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed quarterly and should be at least 8 alphanumeric characters. All default passwords must be changed and all guest or anonymous accounts are prohibited. Authorized users should take steps to prevent unauthorized access to their accounts by logging off when their workstation will be unattended.

Restrictions and Prohibitions on Use and Access

Communications and Internet access should be conducted in a responsible and professional manner reflecting commitment to honest, ethical and non-discriminatory business practice. In furtherance of these goals the following restrictions and prohibitions apply:

Data security

1. Users must safeguard their logon ID and password from disclosure to any person. Users may not access a computer account that belongs to another user. Users must use their own logon ID and password only, are responsible for all activity on their logon ID, and must report any known or suspected compromise of their ID to ADE Network Administration.
2. Unauthorized attempts to circumvent data security schemes; identify or exploit security vulnerabilities; or decrypt secure data are prohibited.
3. Attempting to monitor, read, copy, change, delete, or tamper with another user's electronic communications, files or software without the express authorization of the user is prohibited.
4. Knowingly or recklessly running or installing (or causing another to run or install) a program (such as a "worm" or "virus") intended to damage or place an excessive load on a computer system or network is prohibited.
5. Forging the source of electronic communications, altering system data used to identify the source of messages or otherwise obscuring the origination of communications is fraud and is prohibited.

To promote the efficient use and to avoid misuse of Internet-related systems, a copy of this policy statement will be distributed to and must be accepted by all users. Users are required to familiarize themselves with the contents of this statement.

ADE is responsible for protecting users and the system from abuses of this policy. Pursuant to this duty, the system administrator(s) may take any of the following actions reasonably appropriate to the nature of the offense:

1. Temporary reduction or suspension of computer system privileges.
2. Referral to the offending user's supervisor.
3. Permanent access revocation.
4. For misuse amounting to criminal behavior, referral to appropriate law enforcement agencies.

The ADE as necessary may review sanctions. Alleged violations will be reviewed on a case by case basis.